UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

STEVEN SUMMER and KATELYN VITA, individually and on behalf of all others similarly situated, Plaintiffs, v. AMAZON WEB SERVICES, INC. and CAPITAL ONE FINANCIAL CORPORATION, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiffs Steven Summer and Katelyn Vita ("Plaintiffs"), individually and on behalf of the proposed Class and Subclasses defined *infra*, allege on personal knowledge as to themselves and their own experiences, and on other matters upon information and belief, including the investigation of their counsel.

NATURE OF THE CASE

1. Plaintiffs bring this class action lawsuit against Amazon Web Services, Inc. ("AWS") and Capital One Financial Corporation ("Capital One") for their failure to protect the confidential information of Plaintiffs and millions of other consumers from theft by a malicious hacker. On July 29, 2019, Capital One announced that the sensitive personal information ("SPI")

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

of more than 100 million United States citizens had been stolen from its servers, including names, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, credit scores, credit limits, balances, payment history, contact information, and some transaction data for 2006-2018, as well as bank account numbers and Social Security numbers for approximately 220,000 people.[1]

2. Without greater specificity, Capital One states that small businesses and consumers who applied for credit card products at Capital One between 2005 and "early" 2019 were affected.[2]

3. AWS, a subsidiary of Amazon.com, Inc., is the second-largest cloud computing services provider in the United States by revenue. In 2018, it had more than $25 billion in revenue.[3] Capital One, as of 2017, was the fifth-largest credit card issuer in the United States.[4] Between them, the two are responsible for the transmission of millions of peoples' sensitive personal information each and every day.

4. On July 19, 2019, Capital One determined that the unauthorized access had occurred, and after working with federal law enforcement, announced the arrest of the hacker, one Paige Thompson, on July 29, 2019, concurrent with the breach.[5] AWS stated that "the perpetrator

[1] *See* http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043, last accessed August 12, 2019.

[2] *Id.*

[3] *See* http://techgenix.com/cloud-computing-vendors/, last accessed August 13, 2019.

[4] *See* https://wallethub.com/edu/market-share-by-credit-card-issuer/25530/, last accessed August 13, 2019.

[5] *See* http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

[Ms. Thompson] gained access through a misconfiguration of the web application…" Ms. Thompson was a former employee of AWS.[6]

5. This misconfiguration allowed Ms. Thompson to access the SPI of more than 100 million people and offer it for sale online.

PARTIES

6. Plaintiff Steven Summer is a resident of Nassau County, New York who applied for a Capital One Spark Business credit card on or about March 20, 2018 and was approved. While the card was for Mr. Summer's business, Mr. Summer's credit application provided Mr. Summer's SPI.

7. Katelyn Vita is a resident of Rockingham County, New Hampshire who applied for a Capital One Quicksilver card on or around July 10, 2018 and a Venture One card on or around November 5, 2010. She was approved for both. At the time she applied for both cards, Vita was a resident of Middlesex County, Massachusetts.

8. Defendant Amazon Web Services, Inc. is a wholly-owned subsidiary of Amazon.com, Inc. It is a Delaware corporation with its principal place of business at 410 Terry Ave. N, Seattle, Washington, 98109.

9. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business at 1680 Capital One Drive, McLean, Virginia 22102.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of

[6] https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

the individual class members exceed the sum or value of $5,000,000, exclusive of interest and costs, and this is a class action in which Defendants and members of the proposed plaintiff classes, including the named Plaintiffs, are citizens of different states.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Amazon Web Services, Inc. has its principal place of business in this District, a substantial part of the events giving rise to Plaintiffs' claims occurred here, and Defendant Amazon Web Services, Inc. is a corporation subject to personal jurisdiction in this District and, therefore, resides here for venue purposes.

12. Venue is also proper in this District because a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in and/or emanated from this District.

ADDITIONAL FACTUAL ALLEGATIONS

13. Capital One is a bank holding company which specializes in credit cards and other forms of credit, such as car loans. 75% of Capital One's revenue comes from credit cards.[7] Customers must apply for credit cards to receive them, and Capital One actively solicits potential customers to supply Capital One with their SPI in order to make a determination as to creditworthiness.

14. Capital One uses AWS to store some or all of the SPI of customers and applicants, including Plaintiffs and the Class on cloud-based storage.

15. Cloud-based storage has grown explosively over the past decade as data centers and contracted storage have replaced in-house servers and storage devices.

[7] *See* http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-irhome, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

16. As part of this, Capital One has drastically scaled back its data center usage in recent years as AWS has taken over Capital One's storage needs. AWS notes that, "Capital One selected AWS for its security model…"[8]

17. Part of this security model is Amazon GuardDuty, "a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect…AWS accounts and workloads."[9]

18. Capital One specifically states at the top of its Online & Mobile Privacy Statement that, "Capital One is committed to your privacy. Our goal is to maintain your trust and confidence when handling personal and financial information about you."[10]

19. Further, in its Privacy Frequently Asked Questions ("FAQ") page, Capital One states:

> Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you:
>
> We maintain physical safeguards, such as secure areas in buildings; electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures to protect against ID theft.
>
> We restrict access to information about you to authorized employees who only obtain that information for business purposes.
>
> We carefully select and monitor the outside companies we hire to perform services for us, such as mail vendors who send out our statements. We require them to keep customer information safe and secure, and we do not allow them to use or share the information for any purpose other than the job they are hired to do.[11]

---

[8] https://aws.amazon.com/solutions/case-studies/capital-one/, last accessed August 13, 2019.

[9] https://aws.amazon.com/guardduty/, last accessed August 13, 2019.

[10] https://www.capitalone.com/identity-protection/privacy/statement, last accessed August 13, 2019.

[11] https://www.capitalone.com/identity-protection/privacy/faq, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

20. Similarly, AWS assures its customers (like Capital One) that:

> At AWS, customer trust is our top priority. We deliver services to millions of active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include financial services providers, healthcare providers, and governmental agencies, who trust us with some of their most sensitive information.
>
> We know that customers care deeply about privacy and data security. That's why AWS gives you ownership and control over your content through simple, powerful tools that allow you to determine where your content will be stored, secure your content in transit and at rest, and manage your access to AWS services and resources for your users. We also implement responsible and sophisticated technical and physical controls that are designed to prevent unauthorized access to or disclosure of your content.[12]

21. As stated *supra*, Capital One announced on July 29, 2019 that a hacker, now known to be Ms. Thompson – who was also a former employee at AWS – was able to gain access to Capital One's credit card applicant database and download more than 100 million customer (and potential customer) applications. The Department of Justice referred to the point of access as a "firewall misconfiguration" that "permitted commands to reach and be executed by [a specific server] which enabled access to folders or buckets of data in Capital One's storage space [in AWS]."[13]

22. This firewall is an open-source web application called "ModSecurity."[14] Noted security blogger Brian Krebs notes that the vulnerability in this case was susceptible

[12] https://aws.amazon.com/compliance/data-privacy-faq/, last accessed August 13, 2019.

[13] https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html, last accessed August 13, 2019.

[14] *See* https://en.wikipedia.org/wiki/ModSecurity and https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

to a "well-known" method of hacking called a "Server Side Request Forgery" (or "SSRF"), in which a server can be tricked into running commands it should not be permitted to run.[15]

23. Krebs further noted that:

> "SSRF has become the most serious vulnerability facing organizations that use public clouds," Johnson wrote. "The impact of SSRF is being worsened by the offering of public clouds, and the major players like AWS are not doing anything to fix it. The problem is common and well-known, but hard to prevent and does not have any mitigations built into the AWS platform."
>
> Johnson said AWS could address this shortcoming by including extra identifying information in any request sent to the metadata service, as Google has already done with its cloud hosting platform. He also acknowledged that doing so could break a lot of backwards compatibility within AWS.[16]

24. Other noted security bloggers, such as Evan Johnson of Cloudflare, have noted that SSRF is a "bug hunters [sic] dream" because the attacks are easy to perform and regularly yield critical findings.[17]

25. Johnson further stated that, "[I]t is clear that AWS' product offering is not complete since this is a major and recurring problem amongst their biggest customers. AWS should do something about this because IAM [Identity and Account Management, the permissioned account identity] is the root of all security within AWS."[18]

26. In spite of Capital One and AWS's stated security promises, Defendants failed to live up to their explicit representations regarding the safekeeping of Plaintiffs' and the Class's SPI.

---

[15] *Id.*

[16] *Id.*

[17] https://ejj.io/blog/capital-one, last accessed August 13, 2019.

[18] *Id.*

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

27. Further, neither Capital One nor AWS even discovered the breach until four months after it had occurred.[19] Had Ms. Thompson not publicly spoken about her hack, neither Defendant might have learned of it until much, much later.

28. Following her successful theft of Plaintiffs' and Class members' SPI, Ms. Thompson posted the database containing the SPI to GitHub, a Microsoft-owned collaboration site. It is unknown how long Ms. Thompson left the file there, but it was posted for long enough that at least one person stumbled across it and informed Capital One.[20]

29. It is currently unclear how many others may have downloaded the database and disseminated it to others.

30. Plaintiffs and the Class now face a real, immediate, and continuing risk of identity theft and fraudulent transfers and accounts resulting from Defendants' actions.

31. The processes of discovering and dealing with the repercussions of identity theft and fraudulent payments and accounts are time consuming and difficult. The Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

32. The victims here, Plaintiffs and the Class, are no different, as they are faced with an arduous path to secure their SPI in response to Defendants' negligence. Plaintiffs and the Class must now take the following steps to attempt to prevent further misuse of their SPI:

- Review and monitor bank accounts for any unusual or unknown charges.

[19] http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043, last accessed August 13, 2019.

[20] *See* https://www.wired.com/story/capital-one-hack-credit-card-application-data/?verso=true, last accessed August 13, 2019.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

- Contact their financial institution to determine if there is any suspicious activity on their accounts.
- Change their account information.
- Place fraud alerts on their credit bureau reports.
- Place security freezes on their credit bureau reports.
- Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

33. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when SPI is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

34. In this case, lag time can be years or decades as Plaintiffs' and the Class's information may continue to be available online through third-party bots and search programs.

35. There is a very strong probability that those impacted by Defendants' failure to secure the SPI could be at risk of fraud and identity theft for extended periods of time.

36. As a result of Defendant's negligent security practices, Plaintiffs and the Class have been exposed to fraud and face a heightened and imminent risk of fraud and identity theft. Plaintiffs and the Class must now and in the future closely monitor their financial accounts to guard against identity theft and fraudulent charges and accounts. Plaintiff and the Class may be faced with fraudulent debt or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services and obtaining credit reports, credit freezes, and

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

other protective measures to deter, detect, and mitigate the risk of identity theft and fraud. Some have already incurred costs in doing so.

CLASS ALLEGATIONS

37. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), seeking damages and equitable relief on behalf of the following Class:

> All persons whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.

38. Plaintiff also brings this action on behalf of itself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), seeking damages and equitable relief on behalf of the following Subclasses:

> All Massachusetts residents whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.
>
> All New York residents whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.

39. Excluded from the Class are: Defendants, any parents, affiliates, or subsidiaries of Defendants; any entity in which Defendants have a controlling interest; any of Defendants' officers or directors; any successor or assignee of Defendants; and any entity with whom Defendants contracts for title insurance services. Also excluded is any Judge assigned to this case.

40. The Class is so numerous that joinder of all members is impracticable. While Plaintiff does not know the exact number of the members of the Class, Plaintiff believes it contains at least tens of thousands of members.

41. Common questions of law and fact exist as to all members of the Class. Such questions of law and fact common to the Class include, but are not limited to:

42. Whether Defendants engaged in the wrongful conduct alleged herein;

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

43. Whether Defendants owed a duty to Plaintiffs and members of the Class to adequately protect their SPI;

44. Whether Defendants breached their duty to adequately protect the SPI of Plaintiffs and members of the Class;

45. Whether Defendants should have known that its data systems and processes were vulnerable to attack and taken sufficient steps to prevent such attack;

46. Whether Defendants' conduct, including failure to act, was the proximate cause of, or resulted in, the breach of its database containing SPI;

47. Whether Defendants improperly notified potential victims of the breach at issue in this litigation;

48. Whether Defendants' conduct constituted a violation of New York General Business Law § 349;

49. Whether Plaintiffs and members of the Class suffered legally cognizable damages as a result of Defendants' conduct and are entitled to recover damages; and

50. Whether Plaintiff and members of the Class are entitled to equitable relief.

51. Plaintiffs' claims are typical of the claims of the members of the Class, and Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs and all members of the Class are similarly affected by Defendants' wrongful conduct in that their information was exposed to unauthorized users in violation of federal, state, and common law.

52. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Class. Plaintiffs are represented by counsel who are competent and experienced in the prosecution of security breach and class action litigation.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

53. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

54. Class action treatment is a superior method for the fair and efficient adjudication of the controversy, in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

55. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendants.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of the Plaintiffs and the Class)

56. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

57. Defendants solicited and took possession of the SPI of Plaintiffs and the Class and had a duty to exercise reasonable care in safeguarding and protecting that information from unauthorized access or disclosure. The duty included maintaining and testing Defendants' security systems and taking other reasonable security measures to protect and adequately secure the SPI from unauthorized access and use. Defendants also had a duty to timely notify Plaintiffs and the Class that their SPI had been or may have been stolen. Defendants further had a duty to destroy

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

the SPI of Plaintiffs and the Class within an appropriate amount of time after it was no longer required in order to mitigate the risk of such non-essential SPI being compromised in a data breach. Defendant finally had a duty to take necessary steps to promptly stop any further breach of customer data once Defendants were made aware of the breach.

58. Defendants' duties arose from its relationship to Plaintiffs and the Class and from industry custom.

59. Defendants, through their actions and/or failures to act, unlawfully breached duties to Plaintiffs and the Class by failing to implement standard industry protocols, to exercise reasonable care to secure and keep private the SPI entrusted to it, to notify Plaintiffs and the Class of the breach as soon as Defendant was made aware of it, and to take any necessary steps to immediately end the ongoing breach once Defendants became aware of it.

60. Defendants' failure to exercise reasonable care in safeguarding the SPI of Plaintiffs and the Class by adopting appropriate security measures, including encryption, was the direct and proximate cause of the SPI of Plaintiffs and the Class being accessed and stolen through the data breach.

61. It was foreseeable that if Defendants or their agents did not take reasonable security measures, the SPI of Plaintiffs and the Class would be stolen. Companies like Defendants face a high threat of data breaches due in part to the large amounts and type of information they store and the value of such information on the black market. Defendants should have known to take all reasonable precautions to secure customers' SPI, especially in light of recent data breaches and publicity regarding such breaches.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

62. As a result of Defendants' breach of duties, Plaintiff and the Class have been injured and have suffered damages, including but not limited to time, effort, and money spent monitoring accounts and requesting credit holds, freezes, and checks.

63. Defendants' negligence was a substantial factor in causing harm to Plaintiff and the Class.

64. Plaintiffs and the Class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and any other relief as the Court deems just and proper.

SECOND CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

65. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

66. Plaintiffs and the Class conferred a benefit on Defendants by providing their SPI to Defendants, as well as making monetary payments, in exchange for convenience in the purchase of Defendants' services.

67. Defendants appreciated, accepted, and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiffs and the Class as described herein.

68. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful and inequitable proceeds received by them.

69. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and the Class.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

THIRD CLAIM FOR RELIEF
Violation of New York General Business Law § 349 *et seq.*
(On Behalf of Plaintiff Steven Summer and the New York Subclass)

70. Plaintiff incorporates all prior paragraphs as though fully set forth herein.

71. Defendants are "businesses" within the meaning of N.Y. Gen. Bus. Law § 349.

72. Defendants represented that Plaintiff Summer and the New York Subclass's SPI would be adequately safeguarded when it was not.

73. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer purchasing title insurance from Defendants or their agents. Said deceptive acts and aforementioned practices are material. The solicitation of credit card applications is a consumer-oriented act in that Defendants' web-based services were designed for ease of use for consumer transactions conducted through Defendants' websites, and thereby falls under N.Y. Gen. Bus. Law § 349.

74. A causal relationship exists between Defendants' unlawful conduct and losses suffered by Plaintiff. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and New York Subclass members suffered injury and/or damages.

75. Defendants' wrongful conduct caused Plaintiff and the New York Subclass to suffer an ascertainable loss through the exposure and theft of their SPI. If Plaintiff and the New York Subclass members had been informed about Defendants' actual practices with regard to their SPI, they would not have applied for credit from Capital One.

76. Plaintiff and the New York Subclass members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and attorneys' fees and costs.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

77. Based on the foregoing, Plaintiff Summer and the New York Subclass have been injured in an amount to be determined at trial.

REQUESTS FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court enter judgment against Defendants as follows:

a. Certification of the Class as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. Award Plaintiffs and the proposed Class and Subclasses all available damages, restitution and disgorgement;

d. Award Plaintiffs and the proposed Class and Subclasses equitable and declaratory relief;

e. An order declaring that Defendants' acts and practices with respect to the safekeeping of SPI are negligent;

f. Award Plaintiffs and the proposed Class and Subclasses pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and the proposed Class and Subclasses reasonable attorneys' fees and costs of suit, including expert witness fees; and

h. Award Plaintiffs and the proposed Class and Subclasses any further relief the Court deems proper.

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury.

Dated: August 19, 2019

s/ Dan Drachler
Dan Drachler (WSBA # 27728)
Henry Avery (WSBA # 54086)
ZWERLING, SCHACHTER & ZWERLING, LLP
1904 Third Avenue
Suite 1030
Seattle, WA 98101
Telephone: (206) 223-2053
Facsimile: (206) 343-9636
ddrachler@zsz.com
havery@zsz.com

Liaison Counsel for Plaintiffs and the Proposed Class

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Fred T. Isquith
Matthew M. Guiney
270 Madison Avenue
New York, NY 10016
Phone: (212) 545-4600
isquith@whafh.com
guiney@whafh.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl V. Malmstrom
111 W. Jackson St., Suite 1700
Chicago, IL 60604
Phone: (312) 984-0000
malmstrom@whafh.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on this 19th day of August, 2019, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

s/ Dan Drachler
Dan Drachler, WSBA #27728

Zwerling, Schachter & Zwerling, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101
(206) 223-2053